

DECLARATION OF SENIOR SPECIAL AGENT TIMOTHY WILLIAMS

I, Timothy Williams, Senior Special Agent (SSA) of the United States Secret Service (USSS), assigned to the Raleigh Resident Office of the USSS, pursuant to 28 U.S.C. § 1746 and the laws of the United States, hereby declares under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

INTRODUCTION

1. This declaration is made in support of a complaint to forfeit funds previously seized from three virtual currency (VC) addresses [hereafter collectively referred to as the "Subject USDT Addresses"]. These addresses contained proceeds and/or comingled funds of a cryptocurrency confidence investment scheme, whereby one or more criminal fraudsters used a fraudulent cryptocurrency exchange to commit wire fraud by inducing multiple victims, including but not limited to two victims in the Eastern District of North Carolina identified herein as M.M. and W.M., to send money to VC addresses controlled by the fraudsters. Once they received the VC, it was rapidly transferred to numerous other VC addresses, three of which were subsequently frozen by the USSS. The USSS previously obtained a seizure warrant (Case No. 5:24-MJ-2178-JG) pursuant to 18 U.S.C. § 981(b) to bring traceable proceeds and other comingled funds involved in money laundering into government custody and now submit this declaration to support the funds' forfeiture.

DECLARANT'S BACKGROUND AND EXPERTISE

2. I am a Senior Special Agent (SSA) with the United States Secret Service (USSS) assigned to the Raleigh (NC) Resident Office. I have been employed with the USSS as a Special

Agent since June 2007. I have completed extensive training at both the Criminal Investigator Training Program at the Federal Law Enforcement Training Center, Glynco, GA and the Special Agent Training Course at the USSS training facility located in Beltsville, MD. This training included instruction in general law enforcement and criminal investigations to include violations of Title 18, United States Code, section 1343 (Wire Fraud). During my time with the Secret Service, I have conducted numerous financial crime investigations involving cryptocurrency and other financial instruments.

PURPOSE OF THE DECLARATION

3. I make this declaration in support of the civil forfeiture of the proceeds of a criminal scheme to defraud M.M. and W.M. executed in violation of 18 U.S.C. § 1343 and co-mingled funds that were involved in the unlawful laundering of such property in violation of 18 U.S.C. § 1956. Specifically, this declaration supports the civil forfeiture of the following assets that were previously seized and brought into government custody on December 19, 2024:

- a. 500,002.18 USDT virtual currency (formerly held in address 0xC0c9bAF6bB9b932EEf4a60267aA8c530aF5cb62c) [hereafter “USDT Address A”])
- b. 500,000 USDT virtual currency (formerly held in address 0xf2C678B283B58AC43b9975D13aB3F7cE87422ce0 [hereafter “USDT Address B”])
- c. 500,000 USDT virtual currency (formerly held in address 0xc20DcB6c4Fec2516e21CF52648177721e2744988 [hereafter “USDT Address C”])

As explained below, the foregoing funds represent directly traceable criminal proceeds and/or money involved in the laundering of those proceeds, which were derived from a criminal fraud scheme that successfully defrauded M.M. and W.M. by impersonating legitimate cryptocurrency exchanges and inducing them to transfer VC to addresses belonging to the fraudster(s).

BACKGROUND OF CRYPTOCURRENCY

4. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

- a. *Cryptocurrency and Blockchain Generally:* Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Tether, USD Coin, and DAI. Each unit of cryptocurrency is often referred to as a “coin” or “token.” In general, most cryptocurrencies are considered fungible assets. For example, Bitcoin is considered fungible because each unit of Bitcoin is equivalent to any other unit, meaning they have the same quality and functionality. Regardless of when a unit of Bitcoin was issued (“mined”), all Bitcoin units are part of the same blockchain and have the same functionality. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Users of cryptocurrency use public and private keys to transfer cryptocurrency from one person or place to another. A public key is typically a set of numbers and/or letters that a cryptocurrency user shares with other users to engage in a transaction in

cryptocurrency, whereas a private key is typically a set of numbers and/or letters that the user of an account maintains privately to access his or her cryptocurrency. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. As such, most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.¹ Although many cryptocurrencies are or purport to be pseudonymous, often law enforcement and currency exchangers can use the blockchain to analyze transactions in cryptocurrency, identify individuals who are using cryptocurrency platforms for illicit purposes, and trace fraud proceeds from victims to one or more exchanges or wallets.

- b. *Wallets*: Cryptocurrency is often stored in a virtual account called a wallet, which can exist in, among other forms, an external computer device, a computer, on an application, or online. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. Access to a wallet and the cryptocurrency therein is typically protected by a password only known to the owner or user of the wallet. Wallets can be either “custodial” or “non-custodial” (also referred to as

¹ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

“centralized/decentralized” or “hosted/non-hosted”). In the case of a non-custodial wallet, the owner of the wallet has sole control of the wallet’s private keys, which enable access to the wallet and any funds contained therein. With a custodial wallet, another party controls the private keys to the wallet. This is usually a cryptocurrency exchange, and the relationship between the exchange and the customer can be considered analogous to the relationship between a traditional bank and its customers, where the bank securely maintains funds deposited by a bank customer.

- c. *Exchanges/Exchangers*: Virtual currency “exchangers” and “exchanges” (also referred to as a “Virtual Asset Service Provider” [VASP]), such as Binance, Coinbase, Kraken, and Crypto.com, are individuals or companies that exchange virtual currency for other currencies, including U.S. dollars. Exchanges facilitate the purchase, sale, and transfer of a variety of digital currencies.
- d. *Centralized/Decentralized Exchanges*: Centralized exchanges generally maintain a custodial role for the wallets of its customers, and function as trusted intermediaries in cryptocurrency transactions. Decentralized exchanges consist of peer-to-peer marketplaces where users can trade cryptocurrencies in a non-custodial manner, without the need for an intermediary to facilitate the transfer and custody of funds. Decentralized exchanges are often used to trade, or “swap”, one type of cryptocurrency for another, for which the user pays a transaction fee. Centralized exchanges that conduct business in the United States are required to verify their customers’ identities and abide by Know-Your-Customer/Anti-Money Laundering (KYC/AML) regulations.

- e. *Tether*: Tether, widely known as “USDT,” is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a “stablecoin.” USDT is issued by Tether Ltd., a company headquartered in Hong Kong. Tether is connected to Bitfinex, a cryptocurrency exchange registered in the British Virgin Islands.
- f. USDT is hosted on the Ethereum and Bitcoin blockchains, among others. Ethereum (“ETH”) is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses “smart contract” technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract’s code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum’s distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.
- g. Like other virtual currencies, USDT is sent to and received from USDT “addresses.” A USDT address is somewhat analogous to a bank account number, and is represented as a 26-to 35-character-long case-sensitive string of letters and numbers. Users can operate multiple USDT addresses at any given time, with the

possibility of using a unique USDT address for every transaction. Although the identity of a USDT address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular USDT address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. Unlike bitcoin, one of the most popular cryptocurrencies in use today, USDT is “centralized”, meaning that it is issued and controlled by a governing body. Most other cryptocurrencies are “decentralized” and have no such governing body.

FACTS SUPPORTING FORFEITURE

5. This case concerns a cryptocurrency confidence investment scheme perpetrated on victims throughout the United States, including in the Eastern District of North Carolina. These scams are believed to have originated in China in 2019, and are now mainly operated by organized criminal groups in several countries in Southeast Asia. The scheme often begins when a scammer sends a victim a seemingly innocuous and misdialed text message, or through sending an unsolicited message to a victim’s social media account. From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics similar to those used in online romance scams.

6. Once the victim places enough trust in the scammer, the scammer brings the victim into a cryptocurrency investment scheme. The scammer typically claims to have a technique to quickly make large profits, either through personal expertise with cryptocurrency, or through a trusted relative or friend with insider information. The investment schemes have the appearance

of a legitimate enterprise through the use of fabricated interfaces, derivative websites that appear related to legitimate companies, and other techniques designed to bolster the scheme's legitimacy. This generally includes a fake investment platform operated through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns. The investment platforms are a ruse, and the funds contributed are routed directly to a cryptocurrency address the scammers control. In reality, the victims do not have actual "accounts" at the fake companies – as soon as the victim sends cryptocurrency to the deposit address provided by the scammers, it is immediately moved through many other wallets in order to launder the funds and make them harder to trace. The victims are able to see what they believe are their deposits on the fraudulent website, and the purported large returns on their investments are designed to convince them to invest more.

7. When the victims do attempt to withdraw their funds, they are unable to do so and are often met with various excuses, such as being told they are required to pay "taxes" in order to release their funds. The "tax" payments are an attempt by the scammers to elicit even more money out of the victims. The scammers, in the form of "customer service" for the fraudulent website, will continue to ask for additional payments from the victim, and will not release the funds regardless of how much is paid.

8. In this particular fraud case, two individuals residing in the Eastern District of North Carolina were the victims of a cryptocurrency confidence investment scheme. These individuals were approached and recruited into the scam in different ways, but analysis of the fake investment platforms they were directed to, as well as tracing of the cryptocurrency that they sent, shows that they were likely victimized by the same person or group. The following sections detail the background of each victim's enticement into the scheme. This is followed by a section which

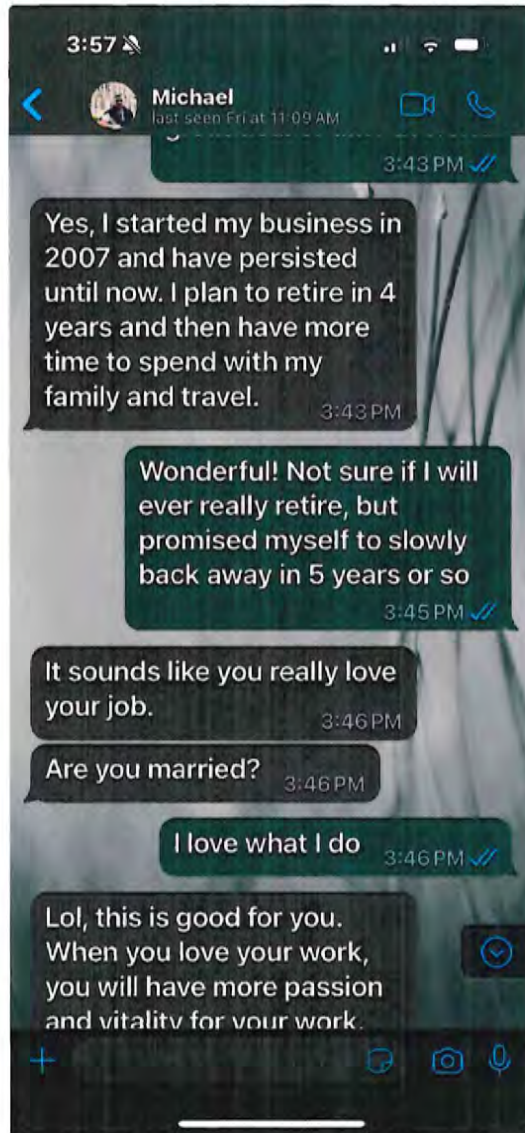
demonstrates the link between the two victims, and shows that there are likely to be many more additional victims of the same group.

FRAUD SCHEME INVOLVING VICTIM M.M.

9. M.M. is a 58 year-old resident of Hampstead, North Carolina. In December 2023 a person claiming to be a man named “Michael Francis” contacted M.M. on the chat application WhatsApp. M.M. had recently asked a friend for investment advice, and this friend said he would have someone reach out to M.M who could provide her with advice. M.M. initially assumed that the message from Francis was this contact. They began a conversation, which initially did not involve investing or cryptocurrency. Francis stated that he wanted to get to know M.M., and they continued a general conversation in this way for approximately two weeks. Francis stated that he lived in San Francisco and owned an import/export company. He claimed to be a widower, and that he had a daughter who lived in Los Angeles with his parents. He sent M.M. numerous photos of himself and his family. These pictures were later found to be taken from the Instagram account of a French fashion designer.



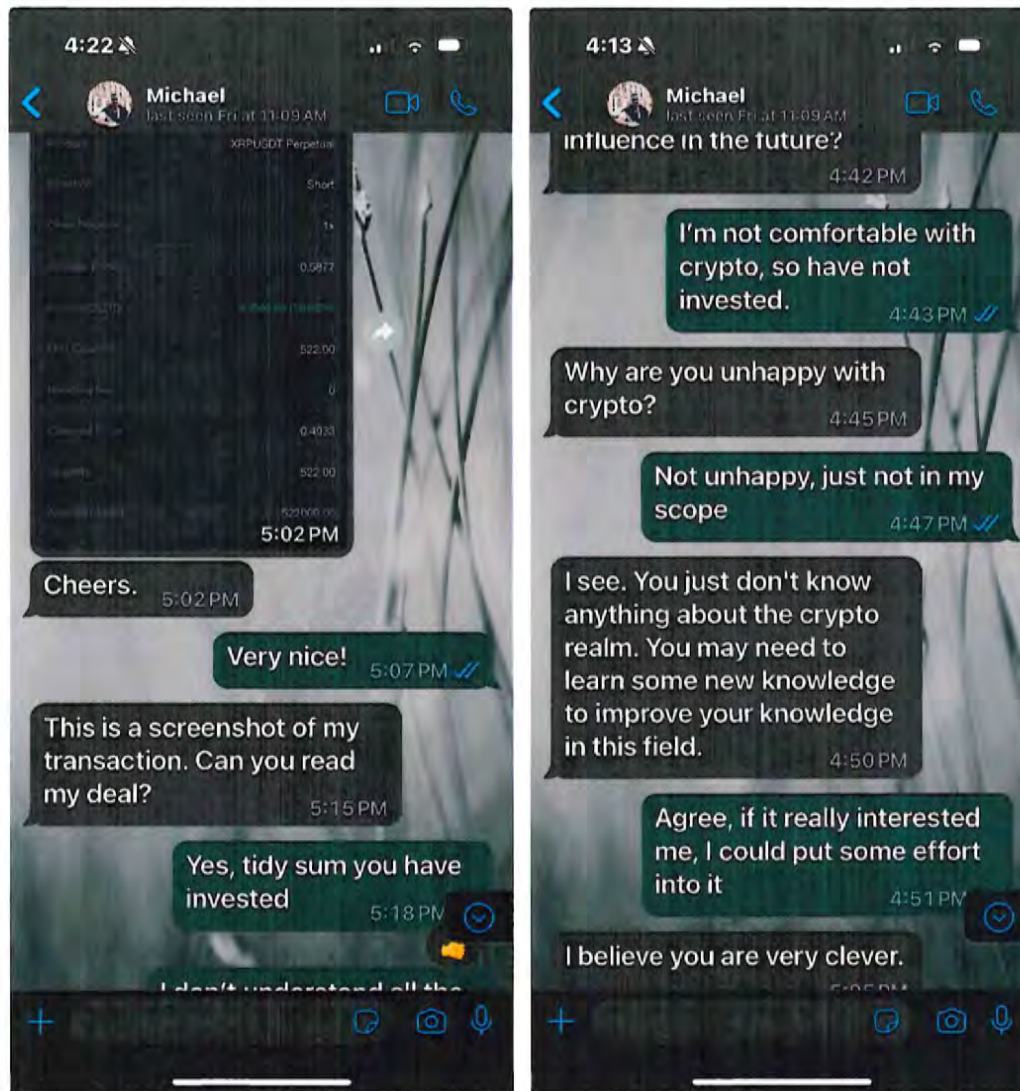
Initial WhatsApp conversation between Francis and M.M.



A sample of the early conversation between Francis and M.M. This is prior to any discussion of crypto or investments.

10. Approximately two weeks into the conversation, Francis brought up financial investments, asking M.M. general questions such as what her financial goals were, when she wanted to retire, and what her current financial situation was. M.M. considered these questions to be normal coming from someone she thought had been asked to provide her with financial advice.

As the conversations progressed, Francis told M.M. that he invested in cryptocurrency and began sending her pictures of his supposed investments, telling her that he was making a lot of money through his cryptocurrency trading. Francis then began to encourage M.M. to try cryptocurrency trading as well, telling her that it was the best way for her to reach her financial goals quickly.

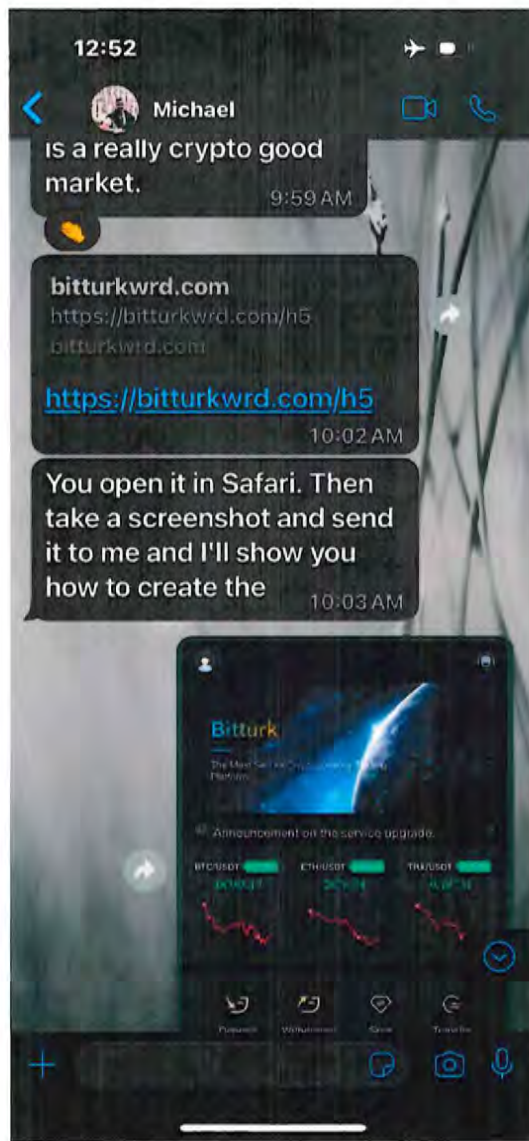


Francis providing a screenshot of his purported crypto transaction, showing a large profit

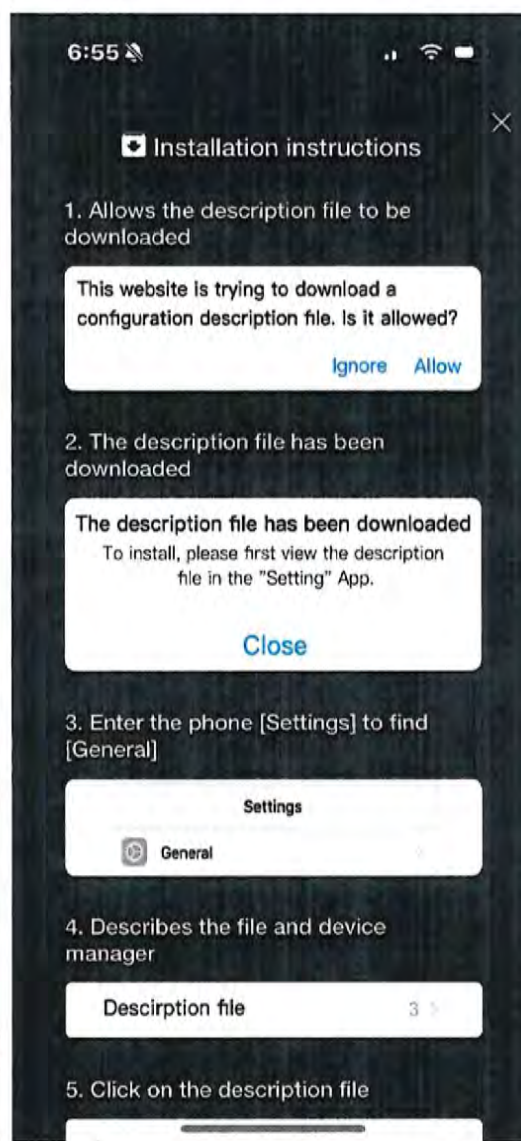
Francis beginning to discuss crypto investments and recommend them to M.M.

11. Francis then began to provide M.M. with specific instructions on cryptocurrency investing, including recommending an investment platform called “Bitturk”. He sent M.M. step-by-step instructions on downloading and installing apps for the legitimate cryptocurrency exchanges Kraken and Crypto.com. At Francis’ direction, M.M. then created accounts at those exchanges, which enabled her to send money from her bank accounts and retirement accounts and convert them to cryptocurrency. Francis also sent M.M. instructions on downloading and setting up the Trustwallet app, which allows users to maintain an unhosted cryptocurrency wallet that is not connected to an exchange. Francis then instructed M.M. in setting up an account at Bitturk, which Francis claimed would allow M.M. to invest in cryptocurrency, at his direction, and receive large profits. There is a legitimate cryptocurrency exchange called “Bitturk”, which has a website at “bitturk.com”. The website that Francis directed M.M. to was “bitturkwrld.com”, which is not connected to the legitimate Bitturk exchange. When Francis told M.M. to install an app on her phone to access her account, instead of having M.M. download it from the Apple App Store, he sent her a link and instructions that enabled a fraudulent Bitturk app to be installed on M.M.’s phone through a process called “sideloading”. Sideloaded apps allow them to be installed on a phone without going through an official app store (either Apple or Google), and also bypasses the security controls and restrictions that normally prevent the installation of malicious or unknown apps. This sideloaded app was not connected to the legitimate Bitturk exchange, which does have an official app that is available on the Apple App Store. In my experience with cryptocurrency confidence investment schemes, this type of step-by-step walkthrough is typical of these cases, as scammers know that they are usually dealing with victims who have little or no prior experience with cryptocurrency, and want to ensure that victims follow their instructions instead of looking

elsewhere for help, which might lead to them realizing they are being scammed. The fraudulent Bitturk app, like most of the fraudulent investment platform apps and websites used in these scams, was created to be fully functional and have all of the capabilities that a victim would expect from an app of this type. Users of the app, including M.M., were able to register for an account, check account balances, trade, and chat with fake Bitturk customer service representatives. The professionalism with which these apps are created is another aspect that leads victims to believe they are dealing with a legitimate trading platform.



Francis recommending Bitturk platform and sending link to download the app



Instructions sent by Francis for installing Bitturk as a "sideloaded" app

12. Once M.M. had completed installing the apps and setting up accounts, as described above, Francis began to guide her through periodic cryptocurrency trades. These were again done in a step-by-step fashion, with Francis sending M.M. a screenshot and instructions for each step in the process. At Francis' direction, M.M. sent money from her bank accounts and retirement accounts to her accounts at Kraken and Crypto.com. Francis also encouraged M.M. to take out a loan to increase the amount of money she could invest. M.M. eventually took out a \$75,000 loan for this purpose. Francis then told M.M. to purchase either Ether (ETH) or Tether (USDT) cryptocurrency from her Kraken and Crypto.com exchange accounts. He then told M.M. to send the ETH or USDT from the exchange accounts to M.M.'s Trustwallet address, which was also under M.M.'s control. From there, Francis instructed M.M. to use the fraudulent Bitturk app to obtain an address for her purported account at Bitturk, which would allow her to send ETH and USDT to her account there. In reality, this address was controlled by the scammers and M.M. never had a legitimate account at Bitturk or any control over the funds once they were sent to this address.

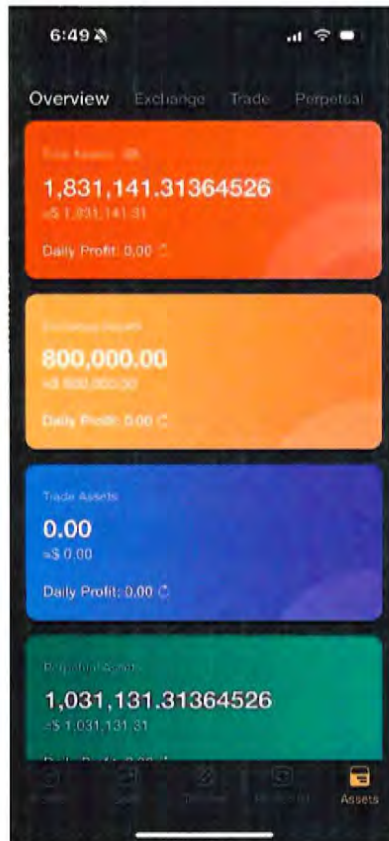


13. Francis would provide M.M. a specific time that each trade would need to be conducted. This timing, as well as the specific trades Francis instructed M.M. to conduct, were supposedly based on Francis' expertise and insider knowledge of cryptocurrency. In reality, the nature of the instructions provided by Francis is not representative of actual cryptocurrency investment or trading techniques. In my experience with these cases, scammers typically provide victims with very specific timing and trade instructions in order to create a sense of urgency (common with many types of scams), as well as to reinforce the supposed expertise of the scammer. Francis told M.M. that following his instructions would provide a high rate of return on

her investment. Following each trade, M.M. was able to see what appeared to be a large profit in her fake Bitturk account. Francis also informed M.M. that she would be able to withdraw funds from her Bitturk account at any time and send them back to her exchange accounts. M.M. followed this process and conducted the first transaction, using the process outlined above, to transfer 0.99 ETH to an address provided by the fraudulent Bitturk app on January 13, 2024.



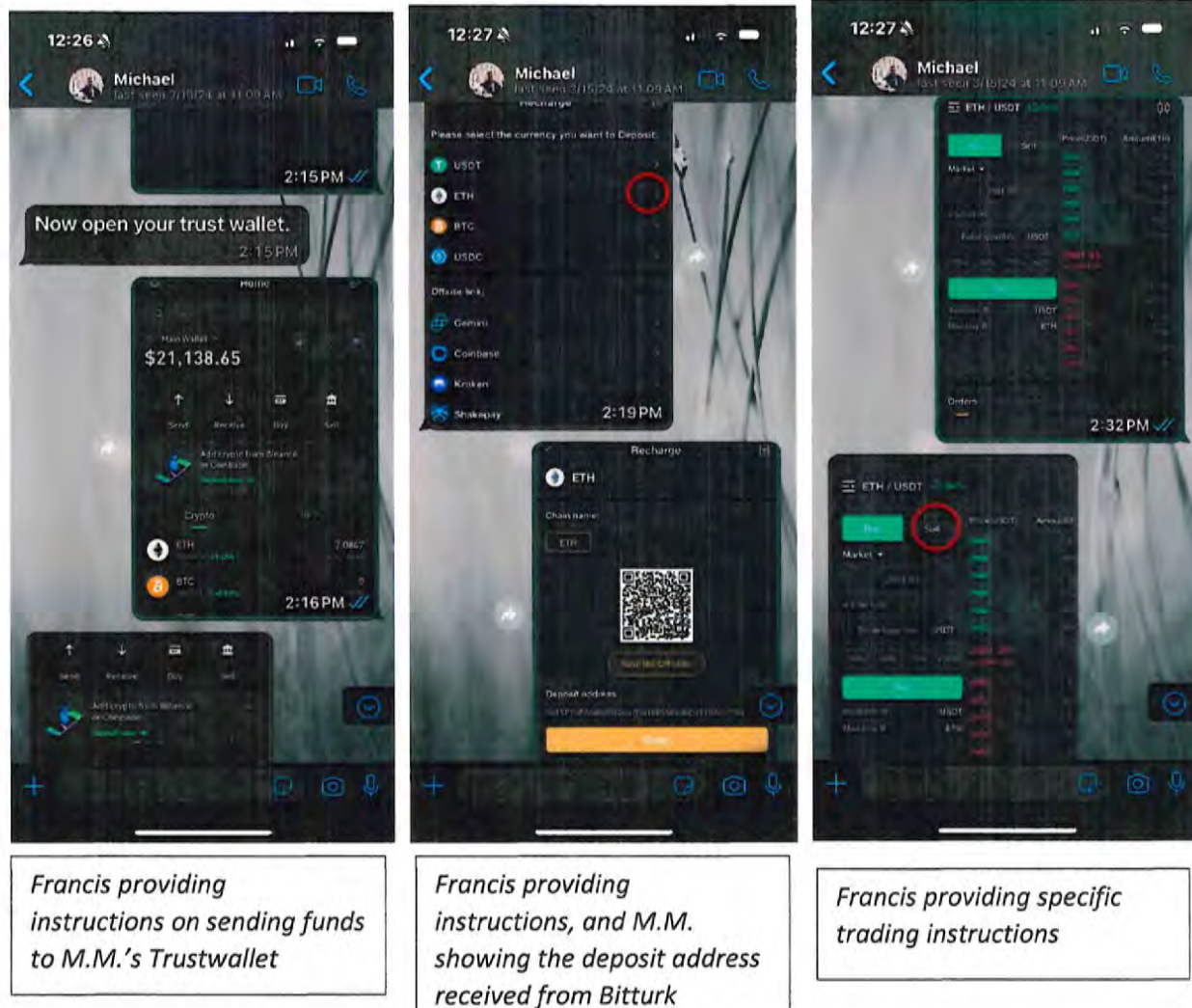
Main page of the Bitturk app



Bitturk app- showing M.M.'s supposed trading profits



Bitturk app- showing a record of M.M.'s trades



14. At Francis' urging, M.M. continued to invest larger amounts, using the same process to transfer a total of approximately 117 ETH and 352,282 USDT from January 13, 2024 to February 24, 2024 (valued at a total of approximately \$669,100 based on the value of the cryptocurrency at the time of each trade). After sending this amount, M.M. attempted to conduct a withdrawal on February 27, 2024. M.M. was told by a fake Bitturk customer service agent that a tax was due on the profits made from her investments. M.M. was also given a timeline to pay the tax, and was threatened with fines, loss of credit score, and other financial and criminal penalties if she did not pay. In my experience, this is a common tactic in the final phase of a

cryptocurrency confidence investment scheme. Victims are told that they need to pay taxes or other fees in order to withdraw their funds, which many do, as they believe they have made a large profit and will gain access to their funds by paying the tax. In this case, M.M. did not have additional funds available to pay the tax, and began to suspect at this point that this was a scam. M.M. reported the situation to the FBI's Internet Crime Complaint Center (IC3) on February 28, 2024, leading to the initiation of this investigation.

Tracing of Victim Funds to the Subject USDT Addresses

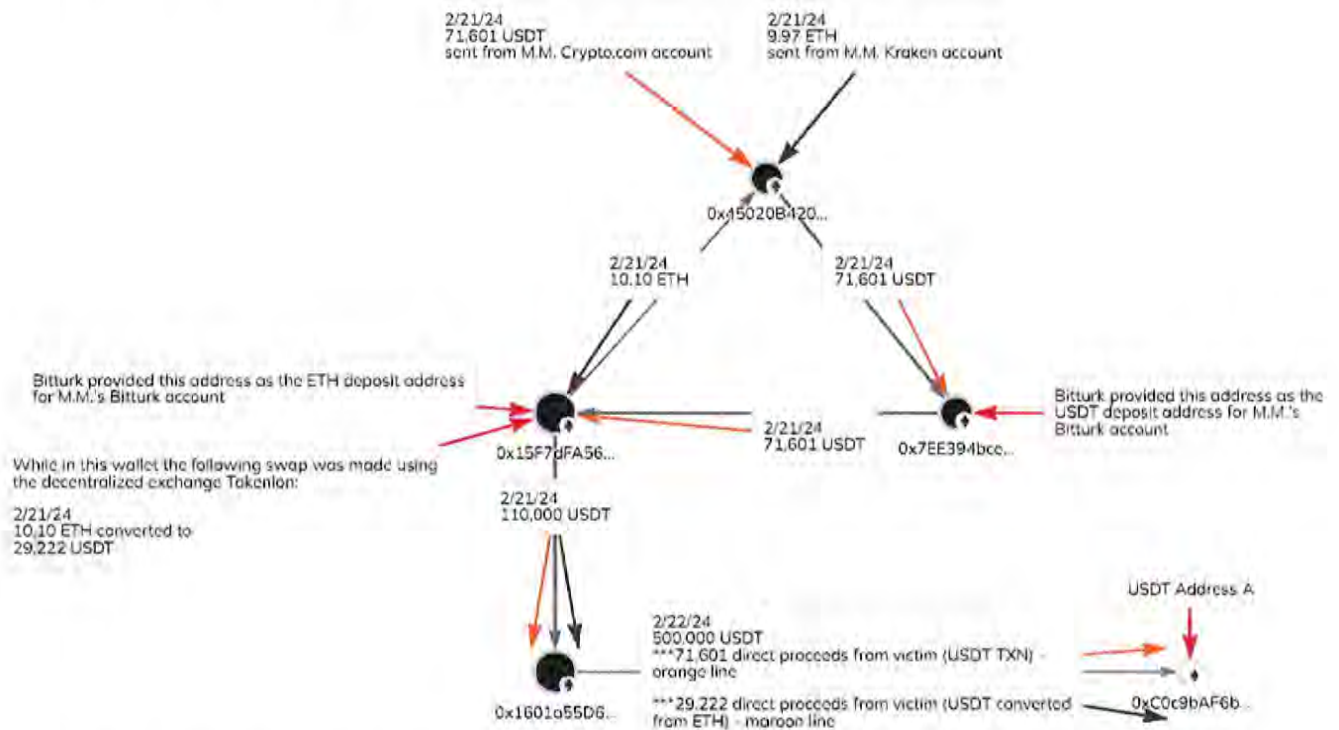
15. Five of M.M.'s cryptocurrency transactions were traced to the Subject USDT Addresses, as detailed below. The traces were conducted using the Last-In-First-Out accounting principle – meaning that the most recently deposited items are recorded as the next withdrawal. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.

16. The following two transactions made by M.M. were traced to USDT Address A:
- a. On February 21, 2024, M.M. sent 71,601 USDT from M.M.'s Crypto.com account to M.M.'s Trustwallet address of 0x45020B. M.M. then sent the 71,601 USDT on to 0x7EE394, which she believed was a deposit address for her Bitturk account. These funds were commingled with additional USDT and ultimately sent to USDT Address A on February 22, 2024 as part of a 500,000 USDT transaction.
 - b. On February 21, 2024, M.M. sent approximately 9.97 ETH from M.M.'s Kraken account to M.M.'s Trustwallet address of 0x45020B. M.M. then sent 10.10 ETH [the 9.97 ETH along with a very small additional amount which had been deposited previously] on to 0x15F7dF, which she believed was a deposit address for her Bitturk account. The 10.10 ETH was then converted to 29,222 USDT using the

decentralized exchange Tokenlon. These funds were commingled with additional USDT and ultimately sent to USDT Address A on February 22, 2024 as part of a 500,000 USDT transaction.

- c. As of March 5, 2024, when the address was frozen by Tether at USSS request, approximately 500,000 USDT was present in USDT Address A, 100,823 of which can be traced as proceeds from M.M.

17. The following is a graphical representation of these transactions:



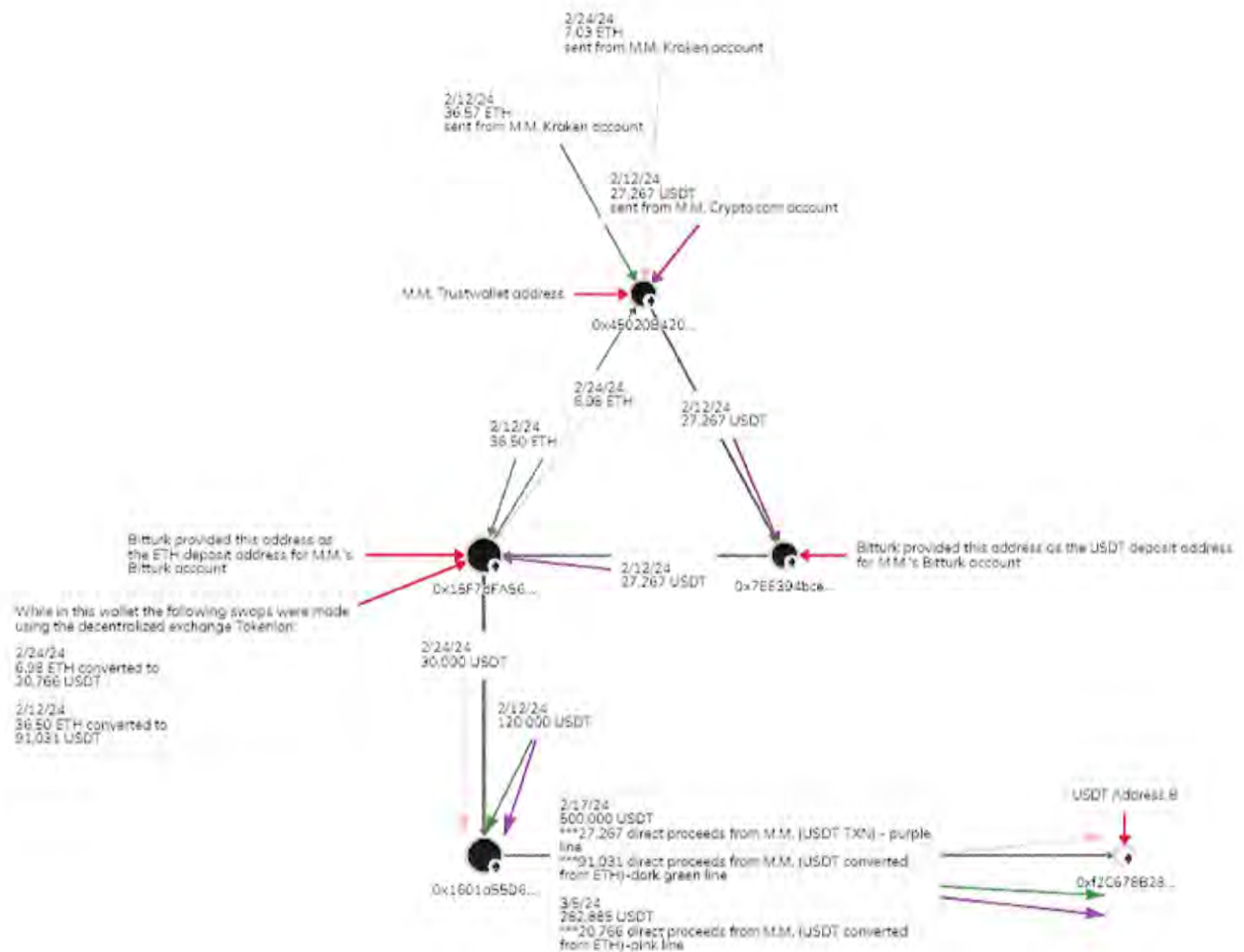
18. The following three transactions made by M.M. were traced to USDT Address B:

- a. On February 12, 2024, M.M. sent 27,267 USDT from M.M.'s Crypto.com account to M.M.'s Trustwallet address of 0x45020B. M.M. then sent the 27,267 USDT on to 0x7EE394, which she believed was a deposit address for her Bitturk account.

These funds were commingled with additional USDT and ultimately sent to USDT Address B on February 17, 2024 as part of a 500,000 USDT transaction.

- b. On February 12, 2024, M.M. sent approximately 36.57 ETH from M.M.'s Kraken account to M.M.'s Trustwallet address of 0x45020B. M.M. then sent 36.5 ETH² on to 0x15F7dF, which she believed was a deposit address for her Bitturk account. The 36.5 ETH was then converted to 91,031 USDT using the decentralized exchange Tokenlon. These funds were commingled with additional USDT and ultimately sent to USDT Address B on February 17, 2024 as part of a 500,000 USDT transaction.
- c. On February 24, 2024, M.M. sent approximately 7.03 ETH from M.M.'s Kraken account to M.M.'s Trustwallet address of 0x45020B. M.M. then sent 6.98 ETH on to 0x15F7dF, which she believed was a deposit address for her Bitturk account. The 6.98 ETH was then converted to 20,766 USDT using the decentralized exchange Tokenlon. These funds were commingled with additional USDT and ultimately sent to USDT Address B on March 5, 2024 as part of a 282,885 USDT transaction.
- d. As of March 5, 2024, when the address was frozen by Tether at USSS request, approximately 500,000 USDT was present in USDT Address B, 139,064 of which can be traced as proceeds from M.M.
- e. The following is a graphical representation of these transactions:

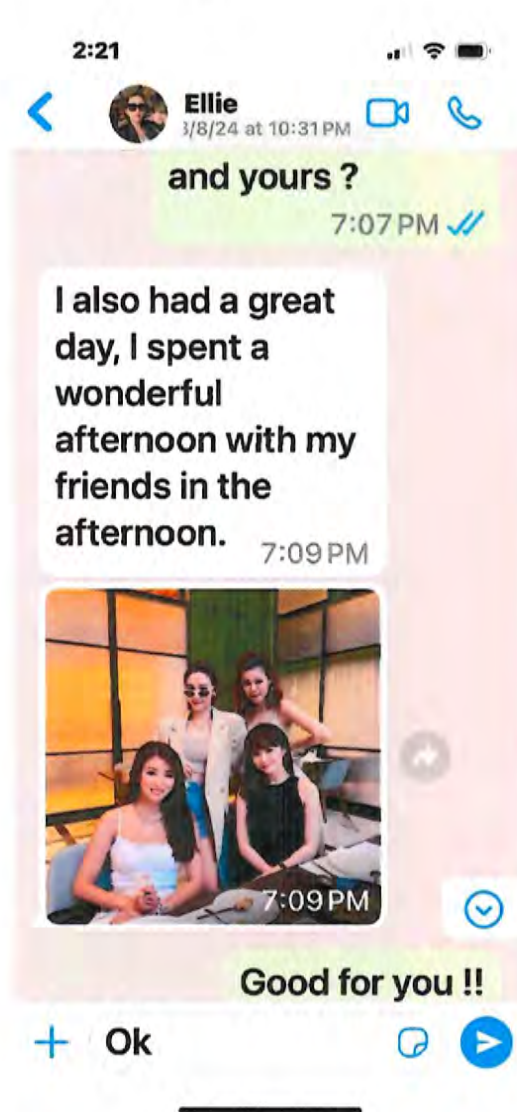
² When ETH, or any token on the Ethereum blockchain, is sent from one address to another, a small amount of ETH is deducted as a "gas fee", which is the term for a transaction fee on Ethereum. This explains why the amount of ETH being sent is slightly less in subsequent transactions.



Fraud Scheme Involving Victim W.M.

19. W.M. is a 60 year-old resident of Fuquay-Varina, North Carolina. In December 2023 a person claiming to be a woman named “Ellie Davis” contacted W.M. on Facebook Messenger. Davis told W.M. that they had spoken before on a dating site. W.M. did not remember speaking to her previously, but then began a conversation with Davis on WhatsApp. This was a general conversation that did not initially involve investing or cryptocurrency. Davis claimed to

live in Los Angeles, that she had a 6-year old son, and that her husband had died of COVID-19 several years ago.



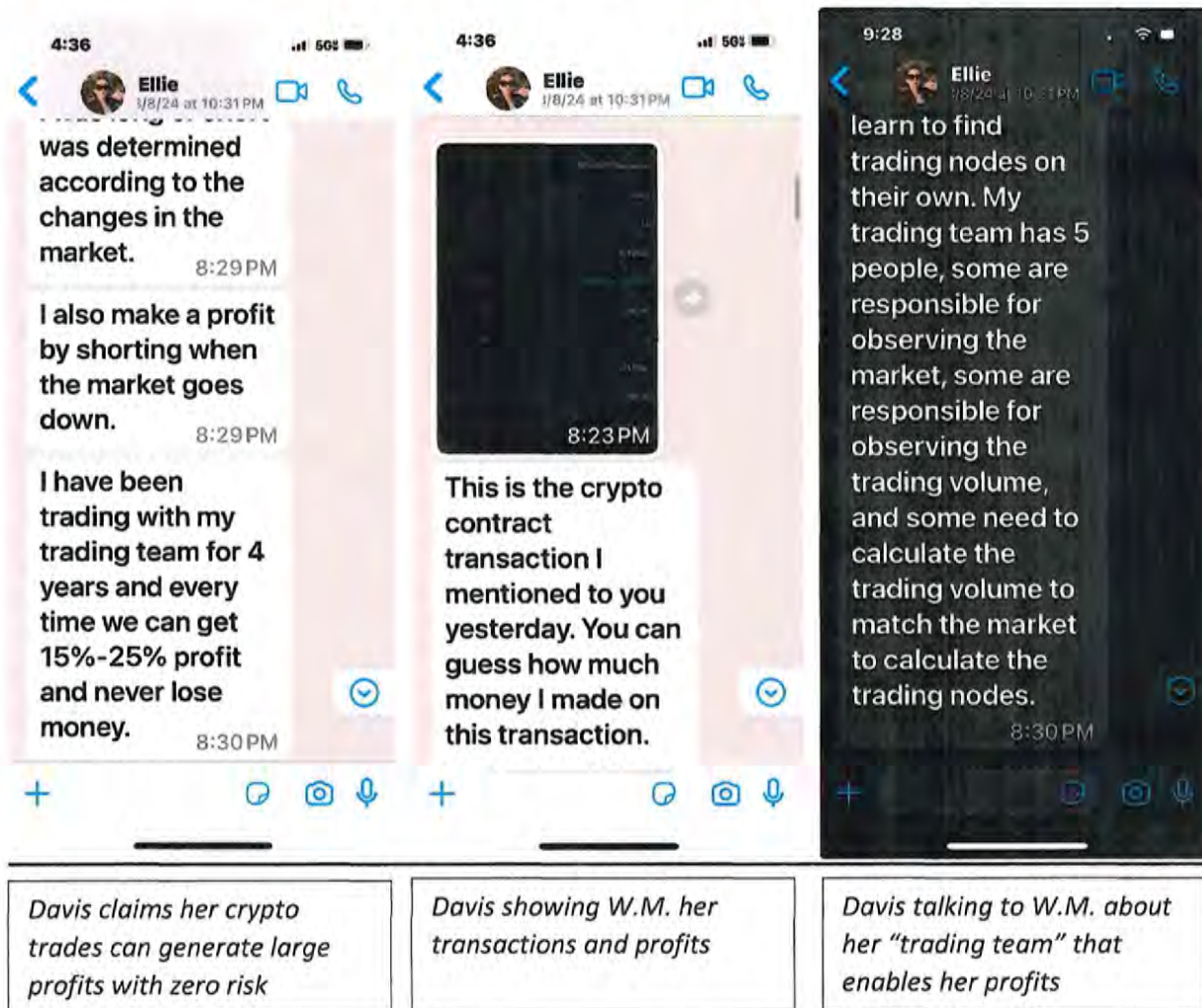
Initial conversations with
Ellie Davis



Initial conversations with
Davis

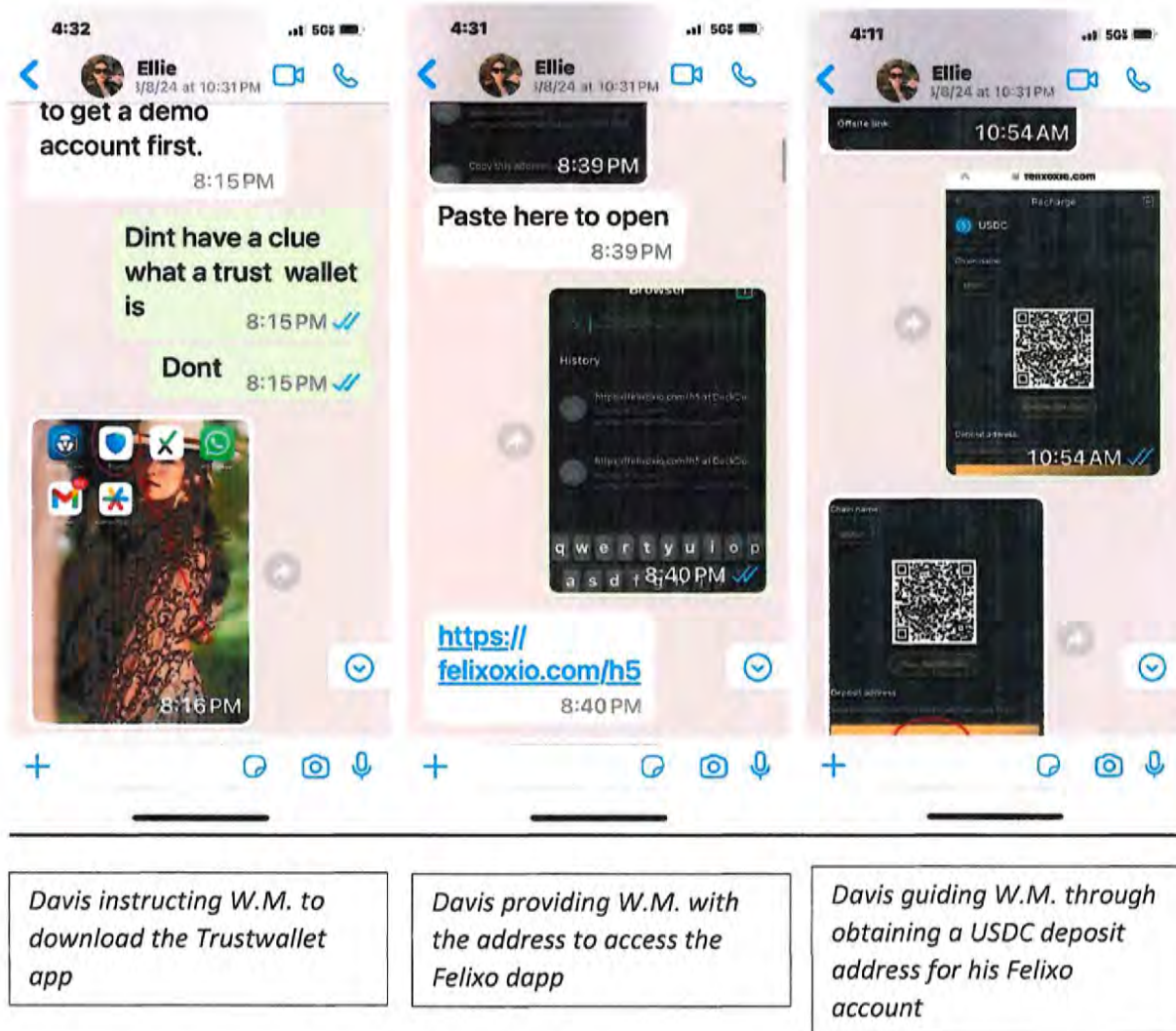
20. After several days of general conversation, Davis brought up investing and asked W.M. if he knew anything about cryptocurrency. Although he had an account at the cryptocurrency exchange Coinbase and had previously bought small amounts of cryptocurrency, W.M. told her that he was not familiar with cryptocurrency trading, and Davis offered to teach him

how to invest and to show him some of her trades and the large profits she was making. She claimed to be making 15-25% profits on a single trade, and after W.M. told her he didn't believe it, she began to send him screenshots of her trades and information on her "trading team" that provided her with analysis in order to make the correct trades without any risk of losing money.

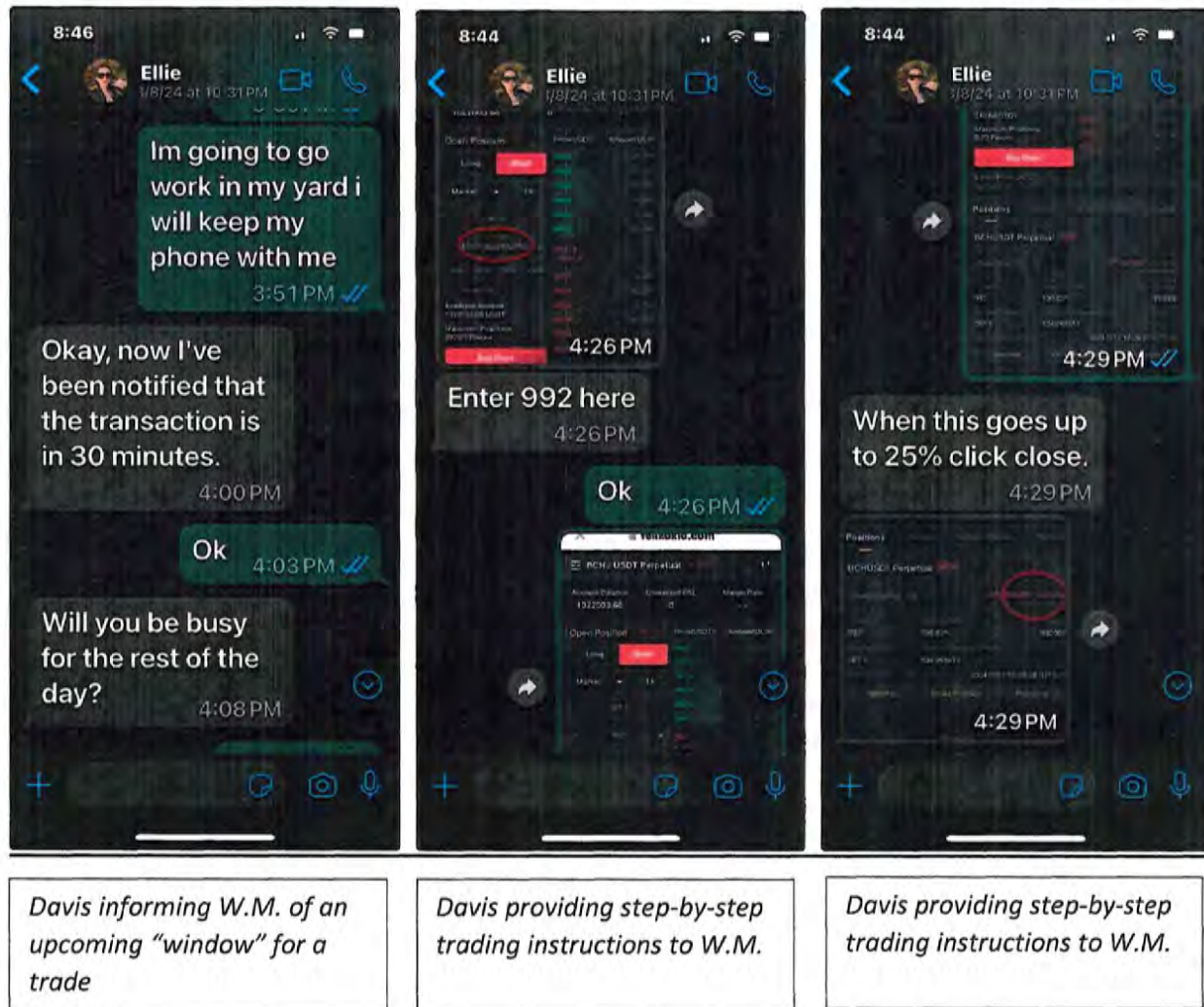


21. Based on the pictures of trades that Davis showed him, W.M. decided to try investing a small amount to see if he could make the same profits. W.M. told Davis multiple times that this was his retirement fund and that he could not afford to lose any of it. Davis assured him that there was zero risk and that he would be able to make enough money to comfortably retire as well as take care of other family members. She recommended that W.M. use a cryptocurrency

trading platform called “Felixo”. There is a legitimate cryptocurrency exchange called “Felixo”, which has a website at “felixo.com”. The website that Davis directed W.M. to was “felioxio.com”, which is not connected to the legitimate Felixo exchange. As Francis had with M.M., Davis guided W.M. step-by-step through the process of setting up the Trustwallet app and an account at the fraudulent Felixo. In this case, Davis did not tell W.M. to set up an unhosted wallet using Trustwallet, but instead used a feature of the app to access the fraudulent Felixo platform through Trustwallet. The Trustwallet app has a browser that lets users utilize decentralized applications, or “dapps.” Dapps are similar to a typical app found on a smartphone, but use blockchain technology to manage user data and maintain it in a decentralized way. On the Trustwallet browser, dapps can be accessed by clicking on icons, or by typing in a specific dapp address, similar to typing in a URL in a web browser. Davis provided W.M. with the address for the fraudulent Felixo and guided him through setting up an account. Once accessed, the fraudulent Felixo dapp had a similar appearance and functionality to a typical cryptocurrency exchange app. Davis then instructed W.M. on how to obtain a deposit address for his fraudulent Felixo account, and then on how to send cryptocurrency from his Coinbase account to this address. As with M.M., this address was controlled by the scammers and W.M. never had a legitimate account at Felixo or any control over the funds once they were sent to this address. The specific cryptocurrency that Davis told W.M. to buy at Coinbase was USD Coin (USDC), which is a stablecoin similar to USDT.



22. Once the process described above was complete, Davis began to guide W.M. through specific trades. As with M.M.'s trades, Davis provided W.M. with a specified time for each trade, along with detailed instructions and screenshots, which told him how to perform the trade in the fraudulent Felixo dapp and what amounts he needed to enter. W.M. followed this process and conducted the first transaction, using the process outlined above, to transfer 2,250 USDC to an address provided by the fraudulent Felixo dapp on December 27, 2023.



23. At Davis' urging, W.M. continued to invest larger amounts, using the same process to transfer a total of approximately 750,774 USDC from December 27, 2023 to February 21, 2024 (valued at approximately \$750,774). On two occasions during this time period, W.M. was able to successfully withdraw small amounts of cryptocurrency from his fake Felixo account back to his Coinbase account. On December 31, 2023 he withdrew 198 USDT, and on February 7, 2024 he withdrew 1,485 USDT. In my experience with cryptocurrency confidence investment schemes, scammers will often allow victims to withdraw relatively small amounts in order to convince them that the investment platform is legitimate. W.M. stated that being able to successfully conduct withdrawals to his Coinbase account was the primary reason that he felt safe to subsequently send

larger amounts of USDC. When he later tried to conduct a larger withdrawal, W.M. was told by a fake Felixo customer service agent that a tax was due on the profits made from his investments. W.M. began to suspect at this point that this was a scam and reported the situation to the Wake County Sheriff's Office and to the FBI's Internet Crime Complaint Center (IC3) on February 27, 2024, leading to the initiation of this investigation.

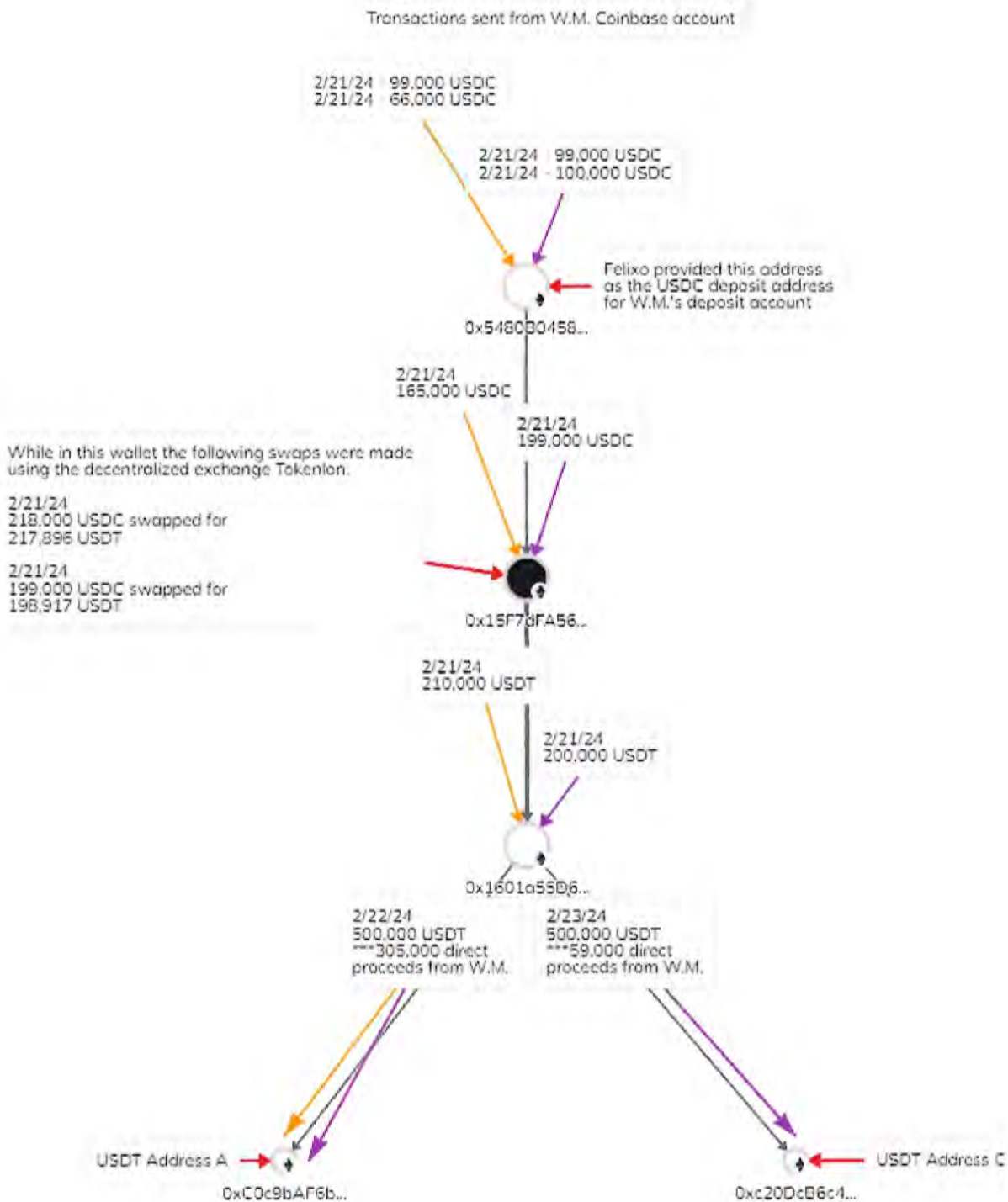
Tracing of Victim Funds to the Subject USDT Addresses

24. Seven of W.M.'s cryptocurrency transactions were traced to the Subject USDT Addresses, as detailed below. The traces were conducted using the Last-In-First-Out (LIFO) accounting principle – meaning that the most recently deposited items are recorded as the next withdrawal. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.

25. The following four transactions made by W.M. were traced to USDT Address A and USDT Address C:

- a. On February 21, 2024, W.M. sent approximately 99,000 USDC from his Coinbase account to 0x5480B0, which he believed was his deposit address at Felixo. These funds were commingled with additional USDC, converted to USDT using the decentralized exchange Tokenlon, and ultimately sent to USDT Address A on February 22, 2024 as part of a 500,000 USDT transaction. Based on the LIFO tracing methodology, a portion of the initial 99,000 USDC transaction was not sent as part of this 500,000 USDT transaction, and was ultimately sent to USDT Address C as part of a 500,000 USDT transaction on February 23, 2024.

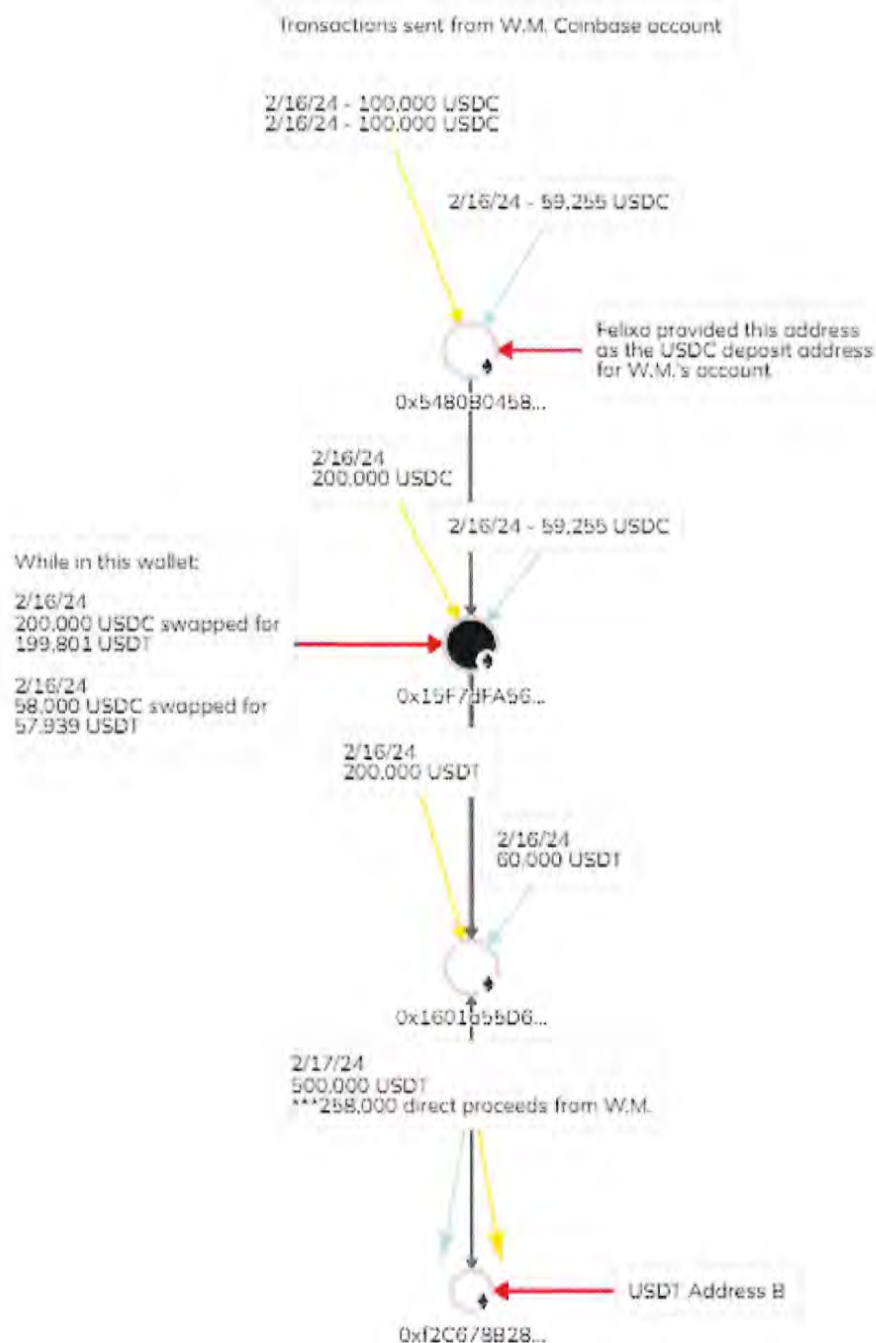
- b. On February 21, 2024, W.M. sent approximately 100,000 USDC from his Coinbase account to 0x5480B0, which he believed was his deposit address at Felixo. These funds were commingled with additional USDC, converted to USDT using the decentralized exchange Tokenlon, and ultimately sent to USDT Address A on February 22, 2024 as part of a 500,000 USDT transaction
 - c. February 21, 2024, W.M. sent approximately 99,000 USDC from his Coinbase account to 0x5480B0, which he believed was his deposit address at Felixo [this is an additional 99,000 USDC transaction from the one described in paragraph 35(a)]. These funds were commingled with additional USDC, converted to USDT using the decentralized exchange Tokenlon, and ultimately sent to USDT Address A on February 22, 2024 as part of a 500,000 USDT transaction
 - d. February 21, 2024, W.M. sent approximately 66,000 USDC from his Coinbase account to 0x5480B0, which he believed was his deposit address at Felixo. These funds were commingled with additional USDC, converted to USDT using the decentralized exchange Tokenlon, and ultimately sent to USDT Address A on February 22, 2024 as part of a 500,000 USDT transaction.
 - e. As of March 5, 2024, when USDT Address A was frozen by Tether at USSS request, approximately 500,000 USDT was present in USDT Address A, 305,000 of which can be traced as proceeds directly from W.M.
 - f. As of March 5, 2024, when USDT Address C was frozen by Tether at USSS request, approximately 500,000 USDT was present in USDT Address A, 59,000 of which can be traced as proceeds from W.M.
26. The following is a graphical representation of these transactions:



27. The following three transactions made by W.M. were traced to USDT Address B:
- a. On February 16, 2024, W.M. sent approximately 59,255 USDC from his Coinbase account to 0x5480B0, which he believed was his deposit address at Felixo. These

funds were commingled with additional USDC, converted to USDT using the decentralized exchange Tokenlon, and ultimately sent to USDT Address B on February 17, 2024 as part of a 500,000 USDT transaction.

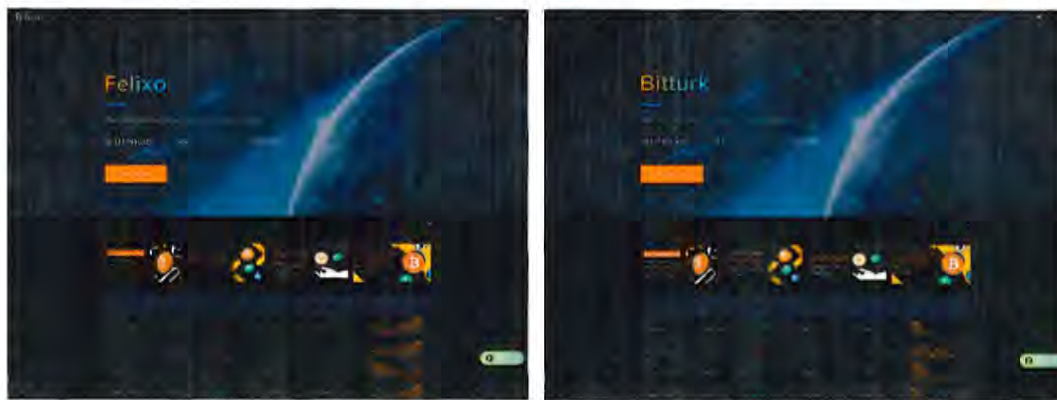
- b. On February 16, 2024, W.M. sent approximately 100,000 USDC from his Coinbase account to 0x5480B0, which he believed was his deposit address at Felixo. These funds were commingled with additional USDC, converted to USDT using the decentralized exchange Tokenlon, and ultimately sent to USDT Address B on February 17, 2024 as part of a 500,000 USDT transaction.
- c. On February 16, 2024, W.M. sent approximately 100,000 USDC from his Coinbase account to 0x5480B0, which he believed was his deposit address at Felixo [this is an additional 100,000 USDC transaction from the one described in paragraph 37(b)]. These funds were commingled with additional USDC, converted to USDT using the decentralized exchange Tokenlon, and ultimately sent to USDT Address B on February 17, 2024 as part of a 500,000 USDT transaction.
- d. As of of March 5, 2024, when the address was frozen by Tether at USSS request, approximately 500,000 USDT was present in USDT Address B, 258,000 of which can be traced as proceeds from W.M.
- e. The following is a graphical representation of these transactions:



28. There are several factors which indicate that the two victims described above are part of a larger fraud scheme. These factors show that the Subject USDT Addresses have been

used not only to launder the proceeds of criminal activity received from M.M. and W.M., but from numerous other victims who are unknown at this time.

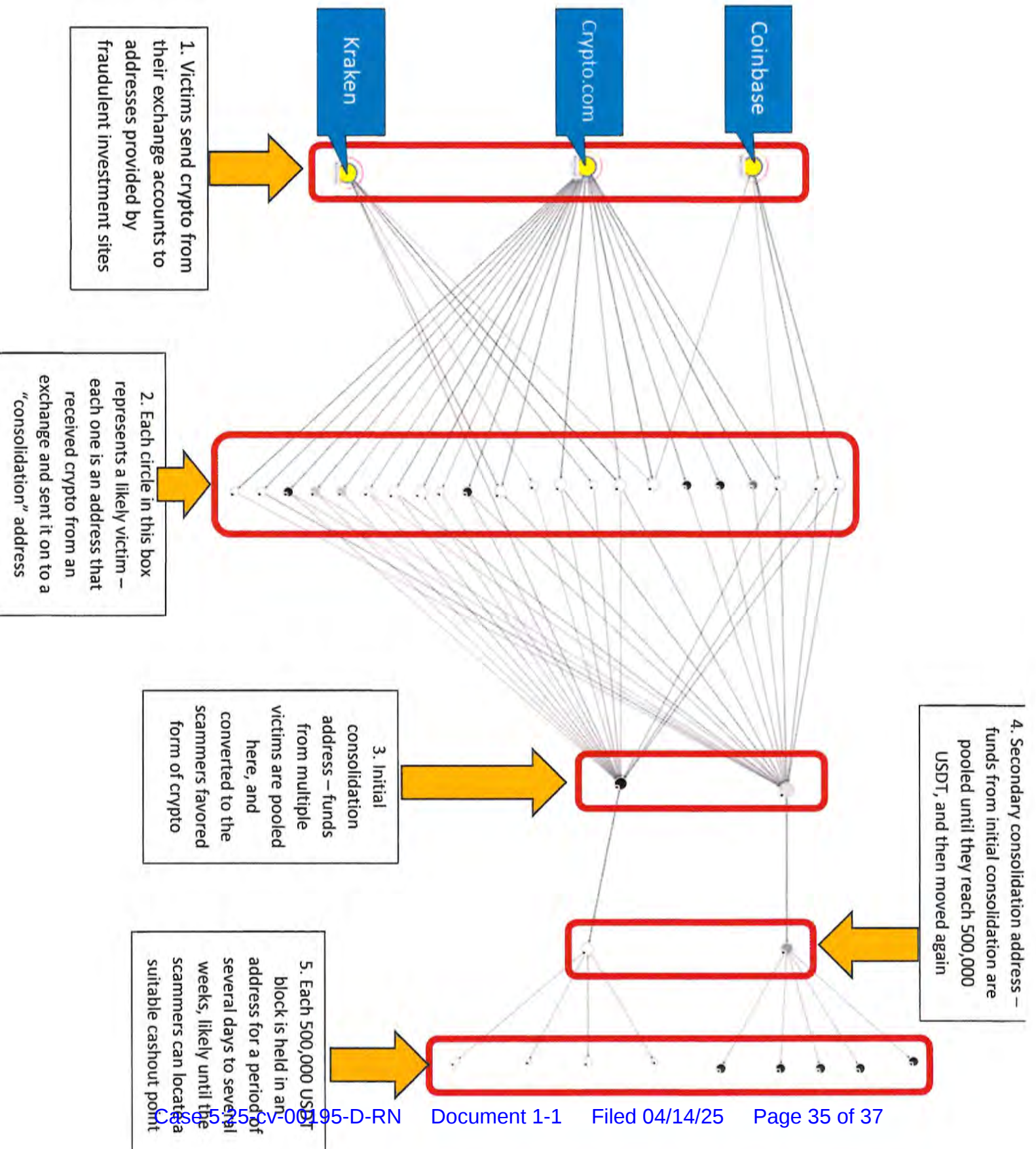
- a. *Fraudulent investment platform website and functionality:* The investment platform websites that the victims in this case were directed to use share a very similar appearance and functionality. An analysis of the source code for each site, conducted by a USSS cyber forensic analyst, determined that they are virtually identical. In addition, an analysis was conducted of both sites using the online tool “URLscan.io”. This tool has the ability to locate “structurally similar” websites by comparing the source code that was used to create a site. When “bitturkwrld.com” and “felixoxio.com” were examined using URLScan.io, 340 structurally similar sites were identified for each of them. The majority of these sites have URLs which suggest they are related to cryptocurrency, and their appearances are identical to the fraudulent sites in this case. Additionally, among the list of structurally similar websites were those with slight variations in the URL from “bitturkwrld.com” and “felixoxio.com”. For example, among the structurally similar sites for “felixoxio.com” are “felixoame.com”, “felixomc.com”, “felixosih.com”, “felixoave.com”, and “felixokl.com”. This is a common tactic in cryptocurrency confidence investment scheme cases, as the scammers want to have backup sites ready to launch in the event the original is shut down by either the domain registrar or hosting company.



Virtually identical fraudulent investment platform websites that M.M. and W.M. were directed to use

- b. *Shared cryptocurrency addresses and patterns of activity:* In cryptocurrency confidence investment schemes, victims are often given individual “burner” VC addresses which are provided only to that particular victim. When a victim sends cryptocurrency to the burner address, the cryptocurrency is then quickly sent to another address where funds from multiple victims are consolidated. There are often multiple layers of consolidation addresses, which can be seen in this case. The tracing of victim transactions in this case showed that all of the transactions which led to Subject USDT Addresses A, B, and C were sent through two “consolidation” addresses, 0x15F7dF and 0x1601a5. Each victim transaction shows a common pattern of moving to an initial consolidation address, where it is converted to what appears to be the scammers’ favored form of cryptocurrency, USDT. The USDT is then sent to a secondary consolidation address, where it is then parceled out into addresses containing 500,000 USDT each. This was the common pattern for every transaction conducted by M.M. and W.M. The chart below illustrates this pattern. This chart was created by “backtracing” from the consolidation addresses that had been identified when tracing M.M. and W.M.’s

transactions. In backtracing, instead of tracing forward to find out where the funds were sent, the analyst traces backwards to see what other addresses had sent funds to the consolidation addresses, and where those funds originated from, which in every case was an exchange. This technique has been found to be very successful in locating additional victims who may not have reported the scam, or may not yet be aware they are a victim. Backtracing from the 500,000 USDT transactions into USDT Addresses A, B, and C indicate at least 20 additional victims of this same fraud scheme.



c. *Other Victim Reporting:* A search of two scam reporting databases, the FBI's IC3 and the Federal Trade Commission's Consumer Sentinel, identified 23 other potential victims of this scam. These victims were located by searching for "Felixo" and "Bitturk" in the databases, as well as for the URLs that M.M. and W.M. used to access those platforms. Each of these victims reported a similar scam to those detailed here, with some variations in how they were recruited for the scam, the name the scammer used when contacting the victim, and the specific URL used to access the platform. Additionally, the Chicago Police Department (CPD) contacted the USSS on November 5, 2024 and provided information on a woman named E.G., who was the victim of a cryptocurrency investment fraud scam. The manner of E.G.'s victimization was very similar to M.M., in that she was contacted by a person named "Michael" who claimed to live in San Francisco, and who eventually directed her to the "Bitturk" investment platform. Analysis and tracing of E.G.'s transactions, conducted by the CPD and verified by the USSS, showed that approximately 100,000 of the 500,000 USDT seized from USDT Address C can be traced as proceeds from E.G.

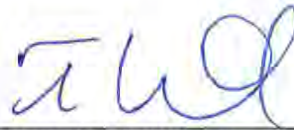
CONCLUSION

29. Based on the foregoing, probable cause exists to believe that the 1,500,002.18 USDT virtual currency (formerly held in USDT Address A, USDT Address B, and USDT Address C) constitutes or is derived from proceeds traceable to a wire fraud scheme executed in violation of 18 U.S.C. § 1343 and/or was involved in money laundering in violation of 18 U.S.C. § 1956,

and is therefore forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and/or 18 U.S.C. § 981(a)(1)(A).

30. The foregoing facts are furthermore sufficient to support a reasonable belief that the defendant property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and/or 18 U.S.C. 981(a)(1)(A).

Executed this 11TH day of April, 2025.



Timothy Williams
Senior Special Agent
United States Secret Service